(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75760 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US00/40137

(22) International Filing Date: 7 June 2000 (07.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/137,885 7 June 1999 (07.06.1999) US
60/170,047 10 December 1999 (10.12.1999) US

(71) Applicant: FIREPAD, INC. [US/US]; The Firepad Building, 625 Ellis Street, Mountain View, CA 94043-2225 (US).

(72) Inventor: MITCHELL, William, E.; 1600 Villa Street, #264, Mountain View, CA 94043 (US).

(74) Agent: ALTMAN, Daniel, E.; Knobbe, Martens, Olson & Bear, LLP, 16th floor, 620 Newport Center Drive, Newport Beach, CA 92660 (US).

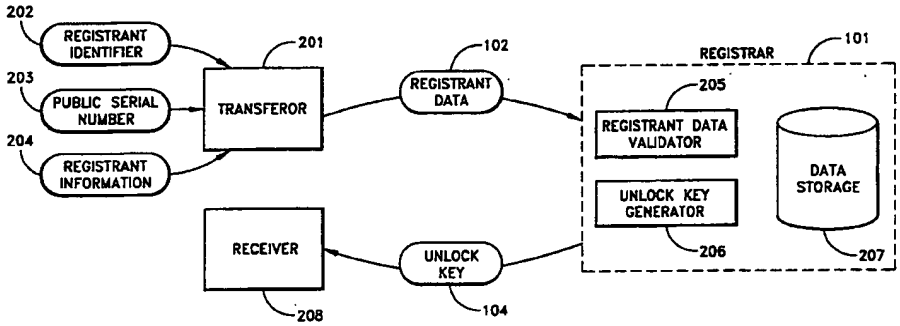
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR PREVENTING THE UNAUTHORIZED USE OF SOFTWARE



(57) Abstract: A system and method are disclosed in which a key for unlocking a target software program is generated (and validated) using information about the end user of the program and/or about a target computing device of the user. The keys are generated by a registrar system, which may be implemented, for example, as an Internet server of a software seller or distributor. Registrant data is initially collected from the user, and/or from a computing device of the user, and is transmitted the registrar system. The registrant data preferably includes (1) a registrant identifier, which may be derived from or contain a username associated with the target device, a unique serial number of the target device, and/or another appropriate identifier of the user or the target device; (2) information about the user, such as the user's name and email address, and (3) a public serial number provided to the user with or in connection with the target software. When the registrar system receives a new registration request, the system initially determines whether some or all of the registrant data is valid. As part of this process, the registration system preferably determines whether the public serial number has been used a maximum number of times. If the registration information is valid, the registrar system generates and returns a key that is specific to the registrant data (and particularly the registrant identifier), and the key is installed on the target device. The target software determines whether the key is valid by determining whether the key corresponds to the registrant identifier (and possibly other registrant data).

WO 00/75760 A1

METHOD AND SYSTEM FOR PREVENTING THE UNAUTHORIZED USE OF SOFTWARE

RELATED APPLICATIONS

This application claims the benefit of both U.S. Provisional Appl. No. 60/137,885, filed June 7, 1999, titled METHOD AND APPARATUS FOR REGISTERING SOFTWARE TO PREVENT UNAUTHORIZED USE, and U.S. Provisional Appl. No. 60/170,047, filed December 10, 1999, titled SYSTEMS AND METHODS FOR ANTI-PIRACY OF DIGITAL INFORMATION, the technical disclosure of which is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to preventing the unauthorized use of a software program. More particularly, the present invention relates to the generation and distribution of an unlock key designed to reduce the unauthorized use of a software program.

BACKGROUND OF THE INVENTION

Software programs are vulnerable to unauthorized copying and use. Software producers loose a significant amount of money as a result of such unauthorized copying and use.

One method of preventing the unauthorized use of a software program is to distribute a locked version of the software program along with an unlock key to be entered into the software program, or into a software installation program. The software program, or the installation program, will not operate fully without the unlock key. This method has weaknesses. For example, this method can be easily circumvented because, once an individual legitimately obtains a copy of the software and an unlock key, that individual can distribute copies of the software and unlock key to others. Further, this method does not allow a software producer to track the use of a particular copy of the software program. Thus, a software producer will have a difficult time, if not impossible time, discerning when unauthorized use of its software programs is occurring. Other copy protection schemes suffer in that they require the end users to attach an electronic security device to the computer. Because of these and other weaknesses in existing copy protection methods, an improved form of prevention is needed.

SUMMARY OF THE INVENTION

The present invention provides a system and method in which a key for unlocking a target software program is generated (and validated) using information about the end user of the program and/or about a target computing device of the user. The keys are generated by a registrar system, which may be implemented, for example, as an Internet server of a software seller or distributor. The invention may be used to register and unlock software programs for PCs, PDAs (personal digital assistants), and other types of target computing devices.

In accordance with the invention, registrant data is initially collected from the user, and/or from a computing device of the user, and is transmitted the registrar system. The registrant data preferably includes the following components: (1) a registrant identifier, which may be derived from or contain a username associated with the target device, a unique serial number of the target device, and/or another appropriate identifier of the user or the target device; (2) information about the user, such as the user's name and email address, and (3) a public serial number

provided to the user with or in connection with the target software. The registrant data may be obtained, for example, by registration software which prompts the end user to enter the appropriate information and/or reads the information from memory. In one embodiment, the registration software runs on a PC or other Internet-connected computing device of the user, and is used to unlock a target program for use on a PDA. In other embodiments, the registration software runs on the target device (e.g., as a component of the target software).

The registrar system includes a database or other data repository which stores information for generating the keys and tracking registration events. This information preferably includes lists of valid public serial numbers (or of private serial numbers associated therewith), and registrant data obtained from end users of the system as the result of registration events. The registrar system also maintains, for each public serial number, a count of the number of times the serial number has been used to register a target program. The count values are used to limit the number of times any given public serial number is used to obtain a key. The limit number may be set by the software seller/distributor to a value (e.g., 2-5) which allows the end user to re-register the target software one or more times (such as when the user purchases a new target device), yet limits the effectiveness of stolen keys to pirates.

When the registrar system receives a new registration request, the system initially determines whether some or all of the registrant data is valid. As part of this process, the registration system preferably determines whether the public serial number is valid, and determines whether the public serial number has been used the maximum number of times. If the registration information is valid, the registrar system generates and returns a key that is specific to the registrant data (and particularly the registrant identifier), and the key is installed on the target device. The key preferably includes an encrypted representation of the registrant identifier. The target software determines whether the key is valid by determining whether the key corresponds to the registrant identifier (and possibly other registrant data). If the key is not valid, the target software is maintained in a locked state.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features will now be described with reference to the drawings summarized below. These drawings and the associated description are provided to illustrate preferred embodiments of the invention, and not to limit the scope of the invention.

Figure 1 illustrates a registration process at a general level.

Figure 2 illustrates a set of components for implementing the registration process.

Figure 3 illustrates the registration process according to one embodiment of the invention.

Detailed Description of the Preferred Embodiments

I. Terminology

As used hereinafter, the following terms have the following meanings (except where specifically indicated otherwise).

The term "target software program" refers to software that an individual or entity seeks to protect from unauthorized use. The target software program may include multiple code modules, including modules that run

remotely from one another. Examples of target software applications include word processing programs, 3D animation programs, spreadsheet programs, online banking programs, operating systems, and controlling systems.

The term "target device" is a device that uses the target program. The target device may be a device used primarily for computing (e.g., a personal computer, a mainframe computer, a handheld computer, and a calculator). The target device may be a device not primarily used for computing (e.g., a household appliance, an automobile, a television set, and a satellite dish) but having components capable of using the target software program. The target program may or may not reside in the target device.

The term "registrant" refers to an individual or entity that seeks to obtain authorized use of the target software program.

The term "register," and its variants refer to the process of obtaining authorized use of the target software program. The registration process may also be used to obtain authorized use of the target device. For example, a target device may be inoperable without the target software program, in which case controlling the use of the target software program has the effect of controlling the use of the target device.

The term "licensor entity" refers to the individual or entity that seeks to protect the target software from unauthorized use..

The term "locked" refers to the state of having a reduced level of functionality. If a software program is locked, the software program may have full functionality for a limited period, limited functionality for an indefinite period, or no functionality whatsoever. A locked software program may be unlocked at which time the software program becomes fully functional. Examples include a word processing program that permits the user to edit documents but not save the documents and a spreadsheet program that does not execute after thirty days of use.

The term "serial number" refers to a value used to identify a license of a software program, a copy of a software program, a license of a device, or a specific device.

The term "end-use" refers to the use of a software program.

The terms "software pirate" or "pirate" refer to an individual or entity that seeks to obtain , or allow others to obtain, unauthorized use of the target software program.

The term "reseller" refers to an individual or entity that seeks to distribute the target software program for a price.

The term "unlock key" refers to a value used to unlock locked software. An entity that controls the distribution of the unlock keys controls the use of corresponding locked software. Typically, the entity wishes to sell the rights to use locked software for a price. Once the price is paid, the entity will distribute the unlock key.

Other terms are introduced and defined throughout the detailed description.

II. Overview

The invention provides a method and apparatus for registering a target software program.

To implement the process, the licensor entity distributes the target software program as locked software ("locked target software"). By distributing the software as locked software, the licensor entity may control the end use of the target software. The licensor entity establishes a system ("registrar") through which a registrant registers the target software program to unlock the target software program. An example of a registrar system is a web server connected to the Internet. In this example, a registrant would be required to visit a web site hosted by the web server in order to obtain an unlock key to unlock the locked target software. An entity or individual that establishes a registrar is a registration entity ("registration entity"). Figure 1 illustrates a registration process at a general level. The registrar 101 receives the registrant data 102. For example, a registrant may enter his name, email address, credit card number, and a serial number into a web page hosted by a web server, functioning as a registrar. The registrar 101, using the registrant data 102, determines whether there is a risk that the registrant 103 is a software pirate. For example, a registrar may comprise a software program capable of recording the number of times a serial number has been used to register the target software program. If the number of times reaches an unacceptable level, the registrar does not send the registrant an unlock key. If the registrar 101 determines that the risk that the registrant 103 is a pirate is sufficiently low, the registrar 101 sends to the registrant 103 an unlock key 104 that will unlock the locked target software. For example, a registrar may comprise a software program capable of recording the number of times a serial number has been used to register the target software program. If serial number had never been used, the registrar emails an unlock key to the registrant. The unlock key 104 is derived from the registrant data 102 in such a way as to hinder the unauthorized use of the target software program. For example, the unlock key could be derived from the serial number of the target device such that the unlock key would not work with other devices with a different serial number. With the unlock key 104, the registrant 103 is able to use the target software program.

Figure 2 illustrates a set of components for implementing the registration process. As depicted in Figure 2, a transferor 201 receives and then transfers the registrant data 102 to the registrar 101. A transferor, for example, may be a web page into which a registrant may enter the registrant data, a software program that prompts the registrant for the registrant data and then communicates via the Internet to the registrar, or an email program that the registrant may use to email the registrant data to the registrar.

As depicted in Figure 2, the transferor 201 obtains certain items, including, but not limited to, a registrant identifier 202, a public serial number 203, and registrant information 204. The registrant identifier 202 and registrant information 204 are, among other things, useful for identifying the registrant and tracking the end-use of the target software program. Examples of a registrant identifier include, but are not limited to, a user-defined username or password, and a unique serial number embedded in a target device and accessible to the transferor. Examples of registrant information include, but are not limited to, the registrant's first name, the registrant's last name, and the registrant's email address. The public serial number 203 is a serial number relating to the target software program. The public serial number 203 is, among other things, useful for tracking the use of a particular license or copy of the

target software program. Examples of a public serial number include, but are not limited to, a serial number printed on a card packaged with a copy of the target software program.

As depicted in Figure 2, the registrar 101 receives the registrant data over the Internet, a dial-in connection, or other communications channel. The registrar 101 consists of a registrant data validator 205, an unlock key generator 206, and data storage 207. The data validator 205 and the unlock key generator 206 are implemented in software, but could alternatively be implemented in-whole or in-part within special hardware.

As depicted in Figure 2, the registrant data validator 205, among other things, accesses the risk that the particular registrant is a software pirate. If the risk that a registrant is a pirate is sufficiently low according to a predetermined algorithm, the registrant data 102 is deemed valid. If the risk that a registrant is a pirate is not sufficiently low according to the predetermined algorithm, the registrant data 102 is deemed not valid. The registrant data validator 205 may evaluate this risk by analyzing the registrant data in context with previously recorded registrant data stored in the data storage, as described below.

As depicted in Figure 2, if the registrant data 102 is valid, the unlock key generator 206 creates an unlock key 104. The unlock key 104 is derived from the registrant data 102 in such a way as to hinder the unauthorized use of the target software program. Examples of the unlock key generator, include, but are not limited to, a software program that derives the unlock key from the registrant identifier.

As depicted in Figure 2, the data storage 207 records information regarding previous registrations and information regarding which public serial numbers are valid. Examples of the data storage include, but are not limited to, a database that contains a record of every valid public serial number, and a database that contains a record of every public serial number that has been registered through the registrar.

As depicted in Figure 2, the registrant data validator 205, an unlock key generator 206, and data storage 207 may reside in a single device or location, or multiple devices or locations. The registrant data validator 205, an unlock key generator 206, and data storage 207 may be implemented by a single individual or entity or multiple individuals or entities. For example, these components could run on a publicly accessible Internet server of a software reseller, or a third party registration entity.

As depicted in Figure 2, the registrar 101 sends and the receiver 208 receives the unlock key 104. Examples of the receiver include, but are not limited to, a software program residing on a computing device that receives the unlock key via the Internet from the registrar. The receiver prepares the unlock key 104 for use with the target software program. Examples of the receiver preparing the unlock key for use with the target software program include the locked target program prompting the registrant for an unlock key and then installing the unlock key, as described below.

III. Detailed Description

The Registrant Identifier

The registrant identifier may be an identifier that is unique for every target device (many devices have a unique serial number). The registrant identifier may also be user-defined (e.g., the HotSync username for a Palm, Inc. Palm(TM) handheld). The registrant identifier may be derived from any unique or non-unique identifier that is defined in software, hardware, or any other means of identification. Regardless of its source, the registrant identifier is used throughout the various embodiments to generate the unlock key, and the unlock key remains useful as long as registrant identifier does not change.

The transferor may obtain the registrant identifier or the user identification number (discussed below) in different ways. For example, a locked version of the target software may display or transfer the registrant identifier or the user identification number to the registrant, who subsequently passes it to the transferor. Alternatively, software other than the locked version of the target software may display or transfer the registrant identifier or the user identification number to the registrant, who subsequently passes it to the transferor. Further, the transferor may obtain the registrant identifier and then create the user identification number. The transferor may obtain the registrant identifier, or the user identification number, through other means not listed.

In another embodiment, for example, the registrant identifier is an identifier that is unique for every target device and the unlock key is derived from the registrant identifier. In this embodiment, the unlock key is only valid for the target device and prevents sharing of the unlock key for pirating purposes. With this embodiment, a new unlock key is obtained from the registrar when the target device is changed (e.g., a customer replaces the target device).

In another embodiment, the registrant identifier is user-defined and the unlock key is derived from the registrant identifier. In this embodiment, the unlock key is valid so long as the user-defined registrant identifier remains the same (e.g., a customer upgrades a Palm handheld, but keeps the same HotSync username). With this embodiment, the registrant obtains a different unlock key when the registrant identifier is changed. Under this embodiment, the unlock key may be used on multiple target devices where the registrant identifier is the same.

A checksum may be generated and transferred as part of the registrant data along with the registrant identifier or the user identification number (discussed below). The checksum is derived from the registrant identifier and/or the user identification number and is used to verify error-free transmission of such data from the transferor to the registrar. The registrar can verify the transmission by deriving the checksum ("derived checksum") in same manner that the original checksum ("original checksum") was derived. If the derived checksum and the original checksum do not match, there was an error in the transmission. This verification process may or may not be performed by the registrant data validator. When the registration process relies on human to transfer the registrant data, the checksum helps to detect errors related to human data entry. For example, a web server, functioning as the registrar, may prompt the registrant for the user identification number that incorporates a checksum. Using the checksum, the

registrar may determine if the registrant correctly types the user identification number. The checksum helps to detect other transmission errors related to the data transfer process.

In one embodiment, a checksum is derived by adding the value of each character in the registrant identifier or the user identification number (discussed below), truncating the total to sixteen bits, translating the truncated total into a four-digit hexadecimal value, translating the hexadecimal value into four ASCII characters, and appending the four ASCII characters to the end of the registrant identifier or the user identification number.

The Registrant Information

The registrant information may include, but is not limited to, the registrant's first name, the registrant's last name, the registrant's email address, the user identification number, the registrant identifier, the credit card number used in the purchase of the target software, an order identification number ("order identification number"), and/or any other information relating to registrant, the registration performed, or the purchase of the target software. The registration information may or may not be included in the registrant data.

The transferor may obtain the registrant information in many ways, including but not limited to, an electronic data transmission, email, web page input, telephone, mail, fax, or shipping.

The Public Serial Number

It is preferred to have a set of unique public serial numbers, which enables the tracking of the use of a particular license or copy of the target software program.

In one embodiment, the public serial numbers are created by encrypting a set of valid private serial numbers. The encryption algorithms referred to herein can be accomplished using any appropriate encryption method, such as methods using private key encryption, public key encryption, symmetric key encryption, or asymmetric key encryption, or a combination thereof. If the public serial numbers are sequential, a pirate could easily derive other valid public serial numbers by obtaining a single public serial number. A pirate could easily obtain a public serial number with a legitimate purchase of the software. Encrypting the private serial numbers to generate the public serial numbers ensures that the public serial numbers are not sequential and are difficult for a pirate to derive without the key.

The transferor may obtain the public serial number in many ways. For example, the registrant may obtain the public serial number through a purchase and subsequently pass the public serial number to the transferor. In a retail store purchase, the public serial number may be provided on a paper certificate or label in a package with or separate from the target software. In an online purchase, the public serial number may be provided by, for example, displaying a customized web page in the registrant's web browser, sending through an electronic data transmission, calling on the telephone, emailing, faxing, mailing, or shipping. In a telephone purchase, the public serial number may be provided by, for example, sending through an electronic data transmission, calling on the telephone, emailing, faxing, mailing, or shipping. Further, the public serial number could be embedded in a software program that is provided to the registrant, such as the target software program or the transferor; this option reduces or eliminates errors related to human entry of the public serial number.

User Identification Number

In one embodiment, an encryption algorithm is applied to the registrant identifier to create a user identification number ("user identification number"). While this encryption algorithm can be accomplished using any appropriate encryption method, it may be a simple transformation. For example, the user identification number may be a hexadecimal representation of the ASCII values of the first six characters of a registrant identifier.

The user identification number can be of any length. The user identification number is included in the registrant data in the place of the registrant identifier. The encryption algorithm preserves the privacy of the registrant by preventing third parties from viewing the registrant identifier. The encryption algorithm deters piracy because the user identification number bears no obvious resemblance to the registrant identifier. Thus, where the unlock key is derived using the registrant identifier, a pirate would not know to alter the registrant identifier to circumvent the protections of the registration process.

The encryption algorithm may be used to transform the registrant identifier into a format supported by most software programs, including, but not limited to, web browsers and email programs. For example, in the embodiment where a registrant enters the registrant data into a web page, it is desirable to have the registrant data to come from character sets supported by the registrant's web browser. However, the registrant identifier may consist of localized character sets (e.g., Kanji and accented Roman characters) that are not supported by the registrant's web browser. The encryption algorithm may be used to transform the registrant identifier from the localized character set into a character set supported by the registrant's web browser. In this embodiment, the user identification number may be a hexadecimal string of ASCII characters. The hexadecimal string of ASCII characters consists of the characters 0 through 9 and a through f which are likely to be supported by most software programs.

The Transferor

In one embodiment, the transferor is a component that a registrant uses to send the registrant data to the registrar. The registrant may send the registrant data to the registrar using any appropriate communications method. Data transfers referred to herein can be accomplished using any appropriate communications methods, such as fax, email, web page input, web page redirect, web page output, telephone, mail, shipping, electronic data transmission, or telephone keypad.

In one embodiment, the transferor is a component that a reseller uses to send the registrant data to the registrar. The reseller obtains the registrant data, excluding the public serial number, using any appropriate communications methods. If the reseller has a set of valid public serial numbers, the reseller transfers to the registrar the registrant data, including a public serial number. Where the reseller has a set of valid public serial numbers, it is preferred that each reseller have a mutually exclusive set of public serial numbers. In this case, either the registrar or the reseller may send the registrant the public serial number for the registrant's records. If the reseller does not have a set of valid public serial numbers, the reseller transfers to the registrar the registrant data, excluding a public serial

number. In this case, the registrar would send the registrant the public serial number, or, alternatively, the registrar would send the reseller the public serial number and the reseller would send the registrant the public serial number.

In one embodiment, the locked target software is the transferor. The locked target software may obtain the public serial number in many ways, including, but not limited to, registrant input or any appropriate communications method. The locked target software may obtain the registrant identifier, or the user identification number (where appropriate), in many ways, including, but not limited to, registrant input or any appropriate communications method. The locked target software may obtain the registrant information, in many ways, including, but not limited to, registrant input or any appropriate communications method. The locked target software may transfer the registrant data to the registrar using any appropriate communications method. In this embodiment, the transferor may reside on the target device or on a device other than the target device. In this embodiment, the transferor may be integrated with a software program that acts as the receiver.

In one embodiment, software other than the locked target software is the transferor. The software other than locked target software may obtain the public serial number in many ways, including, but not limited to, registrant input or any appropriate communications method. The software other than locked target software may obtain the registrant identifier, or the user identification number (where appropriate), in many ways, including, but not limited to, registrant input or any appropriate communications method. The software other than locked target software may obtain the registrant information, in many ways, including, but not limited to, registrant input or any appropriate communications method. The software other than locked target software may transfer the registrant data to the registrar using any appropriate communications method. In this embodiment, the transferor may reside on the target device or on a device other than the target device. In this embodiment, the transferor may be integrated with a software program that acts as the receiver.

The Registrar

The registrar may send the unlock key to the receiver using any appropriate communications method. For example, a registrant may register the target software through a web site, functioning as a registrar. The web site could display a web page that had the unlock key on it. The registrant then could pass the unlock key to the receiver.

In one embodiment, the registrar sends a order identification number to the registrant for the registrant's record keeping.

In one embodiment, the registrar is a component that a reseller operates. In this embodiment, the registrar could be the sole registrar or one of many registrars. In this embodiment, the reseller could be the sole reseller or one of many resellers. In this embodiment, the registrar, a component that a registrant operates, a component that a reseller operates, a component that another reseller operates, the locked target software, or software other than the locked target software may be the transferor. Where a reseller operates both the transferor and the registrar, the transferor functionality and the registrar functionality may be integrated into one software code module or separated into multiple modules. Where a reseller operates both the transferor and the registrar, the transferor functionality and

the registrar functionality may operate on one piece of hardware or location, or multiple pieces of hardware or locations

In one embodiment, the registrar is not a component that a reseller operates. In this embodiment, the registrar could be the sole registrar or one of many registrars. In this embodiment, there could be one reseller, or multiple resellers. In this embodiment, the registrar, a component that a registrant operates, a component that a reseller operates, the locked target software, or software other than the locked target software may be the transferor. Where one entity operates both the transferor and the registrar, the transferor functionality and the registrar functionality may be integrated into one software code module or separated into multiple modules. Where one entity operates both the transferor and the registrar, the transferor functionality and the registrar functionality may operate on one piece of hardware or location, or multiple pieces of hardware or locations.

The Registrant Data Validator

In one embodiment, the registrant data validator determines if the registrant data is valid by comparing the public serial number to a set of valid private serial numbers. If public serial number matches one of the valid private serial numbers, registrant data is valid.

In one embodiment, the public serial numbers are created by encrypting a set of valid private serial numbers. The registrant data validator determines if the public serial number is valid by decrypting the public serial number and comparing the result ("derived serial number") to the set of valid private serial numbers. If the derived serial number matches one of the valid private serial numbers, the registrant data is deemed valid.

In one embodiment, the registrant data validator first compares the public serial number or the derived serial number to a set of valid private serial numbers. If the public serial number or the derived serial number does not match one of the valid private serial numbers, the registrant data is deemed not valid. If the public serial number or the derived serial number matches one of the valid private serial numbers, the registrant data validator determines the number of times that the public serial number has been registered, including the current registration ("total number of registrations"). If the total number of registrations is greater than a predetermined maximum number of registrations allowed ("maximum number of registrations"), the registrant data is deemed not valid. If the total number of registrations is not greater than the maximum number of registrations, the registrant data is deemed valid. By limiting the total number of registrations, the process limits the number of times that a pirate could use a specific public serial number. The total number of times that pirates could use any given public serial number is the maximum number of registrations. Where the maximum number of registrations is one, the public serial number cannot be registered a second time. Where the maximum number of registrations is greater than one, the process provides flexibility for situations when it is desirable to have multiple registrations. It is desirable to have multiple registrations, for instance, when a first registrant purchases the target software out of the box, registers the target software, and then returns the target software for a refund. In that situation, the public serial number is preferably valid for subsequent purchasers. It is also desirable to have multiple registrations when the registrant identifier changes (e.g., the

registrant purchases a new Palm handheld and unlock key is derived from the unique serial number; the registrant alters the HotSync username for a Palm, Inc. Palm handheld). In one embodiment, the maximum number of registrations is three; however, the maximum number of registrations could be any number, including a number which is dependent upon the price or some other attribute of the target software program. When pirates obtain the public serial number, the total number of registrations will likely rise to the maximum number of registrations. This will prevent any pirates from using the public serial number in the future, but this will deprive a legitimate registrant of the benefits of having a maximum number of registrations greater than one. In the case where the registrant had not yet registered the target software, this will deprive a legitimate registrant of initial registration.

In one embodiment, the registrant data validator determines if the registrant information is valid according to conventional methods. If the registrant information is not valid, the registrant data is deemed not valid.

The Unlock Key Generator

The unlock key is derived from the registrant data in such a way as to hinder the unauthorized use of the target software program. The unlock key may be derived from any items or combination of items included in the registrant data.

In one embodiment, the unlock key generator applies an encryption algorithm to the registrant identifier to create the unlock key. Where appropriate, the unlock key generator applies a decryption algorithm to the user identification number to obtain the registrant identifier.

In one embodiment, the unlock key generator applies an encryption algorithm to the concatenation of a registrant identifier and a product identifier ("product identifier") to create the unlock key. The product identifier uniquely identifies the target software program (e.g., a specific version of a particular product). Where appropriate, the unlock key generator applies a decryption algorithm to the user identification number to obtain the registrant identifier.

The Data Storage

The data storage may be accomplished in many ways, including but not limited to, a database.

In one embodiment, the data storage a database that associates a set of valid private serial numbers, or public serial numbers, with a corresponding total number of registrations.

In one embodiment, the data storage is a database that associates a set of registrants with a valid private serial number. The database may also associate certain information with a particular registrant. This information may include any of the registrant data.

In one embodiment, the data storage is a database that contains a set of order identification numbers. The database associates certain information with a particular order identification number. The information may include any of the registrant data.

The Receiver

In one embodiment, the receiver is the locked target software. Examples include, but are not limited to, the locked target software communicating through the Internet with a server, functioning as a registrar.

In one embodiment, the receiver is software other than the locked target software. Examples include, but are not limited to, a software installation program communicating through the Internet with a server, functioning as a registrar.

In one embodiment, the receiver is component that the reseller uses. Examples include, but are not limited to, a reseller web site, functioning as both the receiver and the transferor, which packages the locked target software together with the unlock key for the registrant to download.

The Locked Target Software

The locked target software may be unlocked to create a fully functional, unlocked version of the target software ("unlocked target software"). The locked target software may function with limited functionality that lasts for a limited duration or an unlimited duration. The locked target software may function with full functionality that lasts for a limited duration. After the limited duration of full functionality expires, the locked target software may function with limited functionality that lasts for a limited duration or an unlimited duration.

To unlock the locked target software, the unlock key must be valid. To determine if the unlock key is valid, data ("derived registrant data") is derived the from the unlock key by applying the reverse of the process that the unlock key generator used to create the unlock key. If the derived registrant data matches the registrant data used to create the unlock key, the unlock key is valid. The derived registrant data may include a product identifier, where appropriate.

In one embodiment, the target software program determines if the unlock key is valid only once, at which time the target software program permanently unlocks itself.

In another embodiment, the target software program determines if the unlock key is valid multiple times (e.g., every time the target software program is operated, or once every day that the target software program is operated). In this embodiment, the target software program will function as the unlocked target software if the target software program finds a valid unlock key, and will otherwise function as the locked target software.

When the target software program determines if the unlock key is valid, the target software will look for the unlock key in a predetermined location, such as a location embedded within the target software program, a data file, an expansion file, or an operating system registry.

In one embodiment, the receiver installs the unlock key. In this embodiment, the receiver may determine if the unlock key is valid. If the unlock key is valid, the receiver installs the unlock key; otherwise, the receiver does not install the unlock key. Alternatively, the receiver may simply install the unlock key without verifying the unlock key's validity.

In one embodiment, the locked target software installs the unlock key. For example, the locked target software receives the unlock key after it prompts the registrant for the unlock key. The target software program then places the unlock key in a data file in a predetermined location. The target software subsequently checks for that unlock key in that predetermined location.

In one embodiment, software other than the locked target software and other than the receiver installs the unlock key. For example, a software installation program may be the receiver. In a Palm or other PDA embodiment, for example, the software installation program places the unlock key in a synchronization directory. The software that operates the synchronization is the software other than the locked software and other than the receiver. The software that operates the synchronization then places the unlock key in a data file in a predetermined location. The target software subsequently checks for that data file in that predetermined location.

Distribution of the Target Software Program

The target software program may be distributed in many ways. Additionally, directions to implement the registration process may be given to the registrant by the locked software program, displayed on a web site, or provided to the registrant in a document packaged with the locked target software. The directions will vary with the specific embodiment of the process.

The registrant may purchase a copy of the locked target software packaged with a public serial number printed on a card.

The registrant may purchase a copy of the locked target software in an online purchase and download a copy of the locked target software from a web server.

The unlocked target software may be distributed for use additional to the initially registered use. The copy ("copied target software") of the unlocked target software will need an unlock key to be unlocked. However, where the initial unlock key is derived from registrant data from the initial registration, the initial unlock key may not unlock the copied target software. In that situation, the copied target software will function as locked target software. The individual or entity that obtained the copied target software may seek to register the copied target software and obtain an unlock key. Examples of uses additional to the initially registered use include, but are not limited to, a potential registrant obtains the copied target software from a friend, and an unsuccessful pirate obtaining a copy of the target software program and the first unlock key.

A potential registrant may obtain the locked target software without a public serial number. The locked target software may be offered for download at a reduced price or for free. A copy of the locked target software may be packaged for sale at a reduced price or for free. In this situation, the locked target software may function as a demo version of the software that allows the potential registrant to preview the target software program without paying full price. The potential registrant may seek to register the copied target software and obtain an unlock key.

Integrated Software Package Embodiment

As depicted in Figure 3, in one embodiment, a software package 301 integrates the transferor 201, and the receiver 208. The software package 301 is operated on the computing device 302. The software package, functioning as the transferor 201, obtains the registrant data and transfers the registrant data to the registrar 101 through a data connection 303. If the registrant data is valid, the unlock key is generated. The registrar 101 sends the unlock key to the software package 301, functioning as the receiver 208, through the data connection 303. The software package, functioning as the receiver 208, prepares the unlock key for use with the target software program 304. In this embodiment, the target device may be the computing device 305. For example, the computing device 302 may be a PC, and the computing device 305 may be a Palm handheld or other PDA coupled to the PC by a cradle. In this embodiment, the target device may be the computing device 302. For example, the computing device 305 may be a Palm handheld or other PDA that uses the data connection 303, which may be a wireless data connection or a PC connected to the Internet. In this embodiment, the software package may be downloaded from a reseller's web site, or packaged for retail sale. In this embodiment, the public serial number could be, but need not be, embedded in the software package 301, which reduces errors relating to human input. In this embodiment, a copy of the target software program 304 may be included in the software package 301 initially or may be downloaded through the data connection 303 to the software package 301. In this embodiment, the software package 301 may install the copy of the target software program 304 using any appropriate means. In a Palm or other PDA embodiment, for example, the software package places the unlock key and the target software program in a synchronization directory.

In one embodiment of the Figure 3 system, the software package 301 is provided as a Java applet which runs on a PC 302 in order to register target software for a Palm or other handheld computing device 305. An important benefit to using a Java applet for this purpose is that the software package does not persist on the hard drive or other storage of the PC following installation of the target software. Thus, the registration software does not clutter the user's hard drive, and is not available to pirates or hackers for inspection.

Although this invention has been described in terms of certain preferred embodiments, other embodiments that are apparent to those of ordinary skill in the art are also within the scope of this invention. Accordingly, the scope of the present invention is intended to be defined only by reference to the appended claims.

WHAT IS CLAIMED IS:

1. A method of registering a target software program for use by a user, the method comprising:

receiving registrant data associated with the user and/or a target computing device of the user;

validating the registrant data;

generating an unlock key which is derived from at least a portion of the registrant data, the key adapted to unlock the target software program; and

providing the unlock key to the user.

2. The method as in Claim 1, wherein the registrant data comprises a public serial number, and the step of validating the registrant data comprises determining whether the public serial number has previously been used a maximum number of times.

3. The method as in Claim 2, wherein the maximum number is greater than one.

4. The method as in Claim 1, further comprising installing the key on the target device, and determining, on the target device, whether the key corresponds to the registrant data.

5. The method as in Claim 4, wherein determining whether the key corresponds to the registrant data comprises at least one of (a) determining whether the key corresponds to an identifier of the user, and (b) determining whether the key corresponds to an identifier of the target device.

6. The method as in Claim 1, wherein generating an unlock key comprises applying an encryption algorithm to a registrant identifier contained within the registration data.

7. The method as in Claim 6, wherein the registrant identifier comprises or is based on a username of the user.

8. The method as in Claim 6, wherein the registrant identifier comprises or is based on a serial number of the target device.

9. The method as in Claim 1, wherein validating the registration data comprises:

decrypting a public serial number to create a derived serial number; and

comparing the derived serial number to a set of valid private serial numbers.

10. A method of registering a target software program for use by a user on a target computing device, the method comprising:

obtaining registrant data associated with at least one of the user and the target computing device;

transferring the registrant data to a registrar;

receiving from the registrar an unlock key which is derived from the registrant data; and

unlocking the target software only if the key corresponds to at least a selected portion of the registrant data.

11. The method as in Claim 10, wherein the registrant data comprises a public serial number and at least one of the following: (a) an identifier of the user, and (b) an identifier of the target computing device.

12. The method as in Claim 11, wherein unlocking the target software comprises, at a location of the user, verifying that the unlock key corresponds to at least one of (a) the identifier of the user, and (b) the identifier of the target computing device.

13. The method as in Claim 10 further comprising transferring the target software program and the unlock key from a computer of the user to a target PDA device.

14. The method as in Claim 10, wherein the unlock key comprises an encrypted registrant identifier.

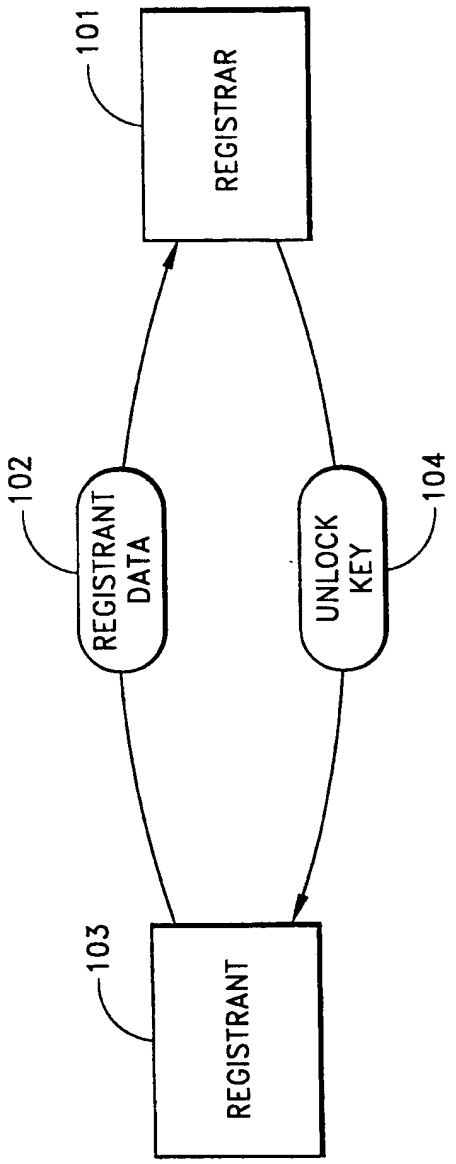

101
REGISTRAR
102
REGISTRANT DATA
UNLOCK KEY
104
103
REGISTRANT

FIG. 1

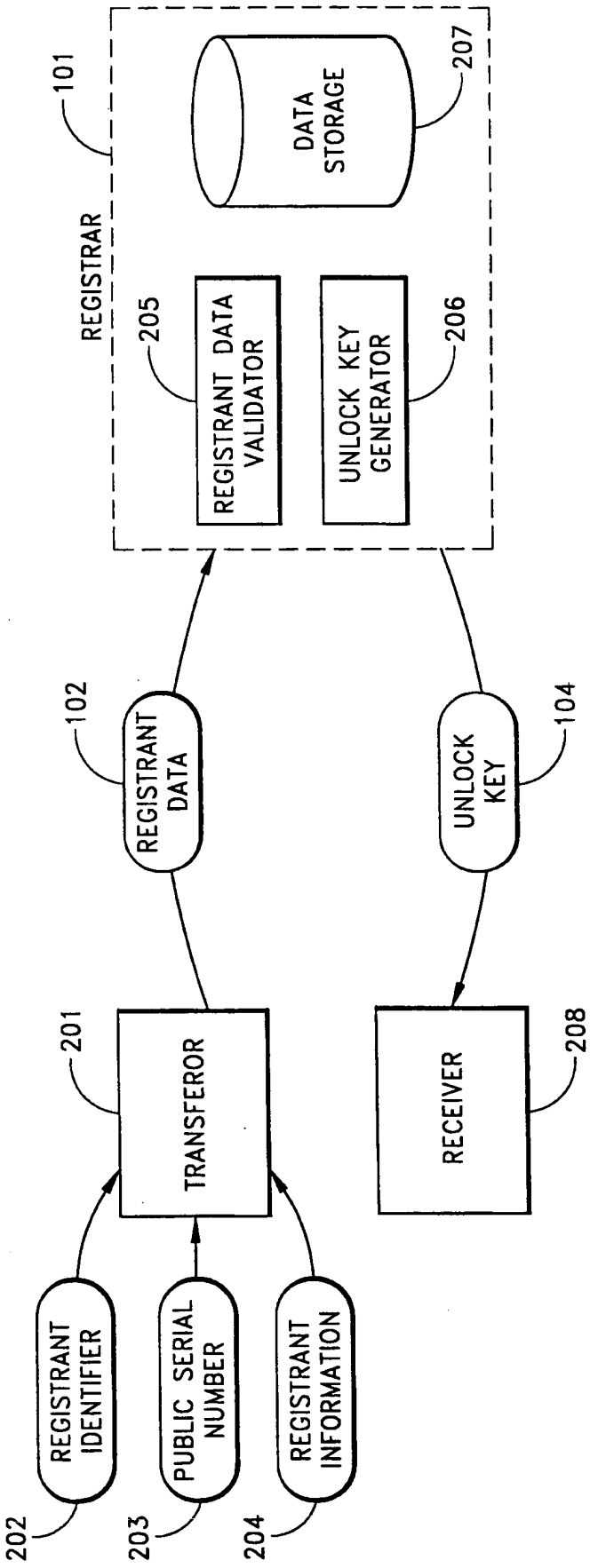

101
REGISTRAR
DATA STORAGE
207
205
REGISTRANT DATA VALIDATOR
UNLOCK KEY GENERATOR
206
102
REGISTRANT DATA
104
UNLOCK KEY
201
TRANSFEROR
208
RECEIVER
REGISTRANT IDENTIFIER
PUBLIC SERIAL NUMBER
REGISTRANT INFORMATION
202
203
204

FIG. 2

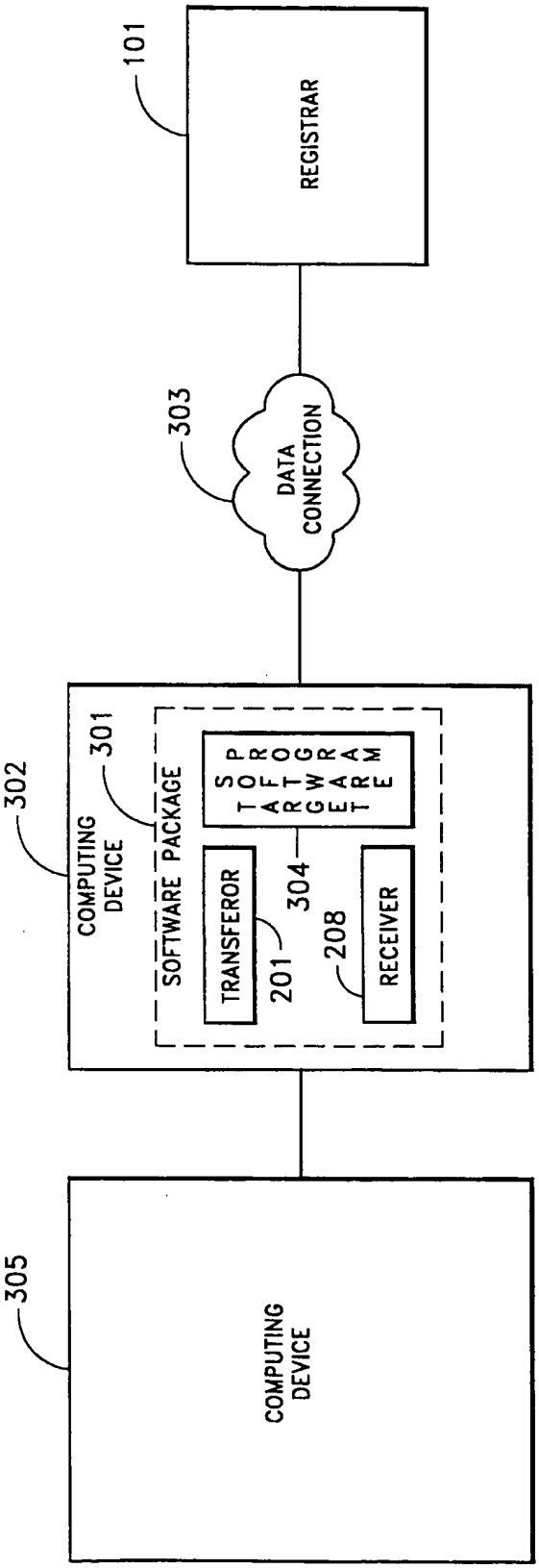

101
REGISTRAR
303
DATA CONNECTION
302
COMPUTING DEVICE
301
SOFTWARE PACKAGE
SPTOARFTOGWRAATRME
TRANSFEROR
201
304
208
RECEIVER
305
COMPUTING DEVICE

FIG. 3

INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/US 00/40137

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 679 980 A (IBM) 2 November 1995 (1995-11-02) abstract; figures 5,8-17 column 10, line 3 - line 52 column 11, line 45 -column 12, line 13 column 13, line 48 -column 15, line 39 column 18, line 10 -column 21, line 14	1,4-8, 10-12,14
Y	---	2,3,9
X	EP 0 766 165 A (FUJITSU LTD) 2 April 1997 (1997-04-02) abstract; figure 1 column 5, line 25 - line 29 column 7, line 20 -column 11, line 45	1,4-8, 10-12,14
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 August 2000	21/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/40137

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 11478 A (SUBBIAH SUBRAMANIAN; LI YANG (US); RAO D RAMESH K (US)) 19 March 1998 (1998-03-19) abstract; figure 5 page 3, line 12 -page 5, line 9 page 9, line 26 -page 11, line 6	2,3
Y	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) abstract; figures 1,14 page 5, line 16 -page 8, line 22 page 23, line 10 -page 25, line 15 page 26, line 29 -page 27, line 17 page 33, line 5 -page 34, line 11	9
A		2,3
A	EP 0 689 120 A (AT & T CORP) 27 December 1995 (1995-12-27) abstract; figure 1 column 3, line 58 -column 5, line 5	13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 00/40137

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0679980 A	02-11-1995	US 5757907 A	26-05-1998
		BR 9501522 A	21-11-1995
		CA 2145926 A,C	26-10-1995
		JP 7295801 A	10-11-1995
		KR 200443 B	15-06-1999
EP 0766165 A	02-04-1997	JP 9069044 A	11-03-1997
		CN 1149219 A	07-05-1997
		US 5935243 A	10-08-1999
WO 9811478 A	19-03-1998	US 6035403 A	07-03-2000
		AU 4341697 A	02-04-1998
		EP 0925536 A	30-06-1999
WO 9842098 A	24-09-1998	AU 6759198 A	12-10-1998
		EP 0968585 A	05-01-2000
EP 0689120 A	27-12-1995	US 5802275 A	01-09-1998
		JP 8016387 A	19-01-1996
		SG 33359 A	18-10-1996